



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/624,923	07/25/2000	Stuart D. Green	JTT006-00	7085

7590 02/10/2004

JEFFREY VAN MYERS
P.O. BOX 130
DRIFTWOOD, TX 78619

EXAMINER

REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 02/10/2004

3

Please find below and/or attached an Office communication concerning this application or proceeding.

pley

Office Action Summary

Application No.

09/624,923

Applicant(s)

GREEN ET AL.

Examiner

Christopher A. Revak

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 October 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: On page 1, in the section titled "Cross reference to related applications", reference is made to Application Serial No. 09/332,795. The current status of the application is not listed and should be amended to indicate that the application has become abandoned.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-4,9-13,18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al, U.S. Patent 5,968,176 in view of Sheldon.

As per claims 1,10, and 19, it is recited by the teachings of Nessett et al of system and method for establishing a firewall system in a network that has security functions (col. 3, lines 20-22 and col. 5, lines 58-60). The teachings are embodied as a WAN that connects private (trustworthy) networks across the Internet (untrustworthy network)(col. 10, lines 28-31 and col. 15, lines 22-26). A network management station (server) includes a topology database that stores the security policy statements

(protection rules)(col. 7, lines 13-21). The security policy statements (protection rules), when applied, identify the traffic (communications transactions) of a particular type of selected communication transaction and how the firewall (portal) should behave (col. 3, lines 29-34, col. 10, lines 1-9, & col. 17, lines 32-40). A firewall (portal) is connected between the Internet (untrustworthy network) and the private (trusted) network (col. 3, lines 20-27 & col. 10, lines 28-31). Updates to the security policy statements (protection rules) are selectively transferred from the network management station's (server) database to the firewalls (portals) across the Internet (untrustworthy network)(col. 9, lines 17-32 & col. 10, lines 28-31). The teachings of Nessett et al disclose of controlling network traffic (col. 3, lines 53-54) and that a security policy dictates the way the network devices should accept or deny traffic (communication transaction) according to the firewall (portal)(col. 17, lines 32-40), but the teachings of Nessett et al are silent in disclosing that the transfer of selected communication transactions from an untrustworthy network is prevented. It is disclosed by Sheldon that a firewall enforces security policies by monitoring traffic from outside the network such as the Internet (untrustworthy network) addressed to the internal network (trustworthy network) and selectively preventing the transfer of traffic (communication transactions) by applying security policies (protection rules)(pg 3 & 7). It would have been obvious to a person of ordinary skill in the art to have been motivated to apply means to prevent the transfer of communication transactions from an untrusted network as a means of protecting a trusted network from a malicious attack. Sheldon recites motivation for the use of firewalls implementing security policies to prevent the transfer of communication

Art Unit: 2131

transactions from untrustworthy network whereby it is taught that firewalls keep hackers out of your network by monitoring for attacks and when one is detected, action is taken to prevent it from happening (pg 4). Although the teachings of Nessett et al disclose of the use of a firewall that enforces a security policy, it is obvious that the teachings of Nessett et al utilize the firewall as a measure to prevent the transfer of communication transactions from untrusted networks to a trusted network as is notoriously well known in the art and as evidenced by the teachings of Sheldon.

As per claims 2 and 11, it is disclosed by Nessett et al that the communication of information across the WAN uses cryptography (secure protocol)(col. 16, lines 21-24). Updates to the security policy statements (protection rules) are selectively transferred from the network management station's (server) database to the firewalls (portals) across the Internet (untrustworthy network)(col. 9, lines 17-32 & col. 10, lines 28-31).

As per claims 3 and 12, Nessett et al teaches of security policy statements (protection rules), when applied, identify the traffic (communications transactions) of a particular type of selected communication transaction and how the firewall (portal) should behave (col. 3, lines 29-34, col. 10, lines 1-9, & col. 17, lines 32-40). A firewall (portal) is connected between the Internet (untrustworthy network) and the private (trusted) network (col. 3, lines 20-27 & col. 10, lines 28-31). Updates to the security policy statements (protection rules) are selectively transferred from the network management station's (server) database to the firewalls (portals) across the Internet (untrustworthy network)(col. 9, lines 17-32 & col. 10, lines 28-31). The teachings of Nessett et al disclose of controlling network traffic (col. 3, lines 53-54) and that a

Art Unit: 2131

security policy dictates the way the network devices should accept or deny traffic (communication transaction) according to the firewall (portal)(col. 17, lines 32-40). It is interpreted by the examiner that the teachings of Nessett et al select between two classes for security policies (protection rules) when applied to monitoring traffic, namely an exclusion class that denies network traffic (communication transaction) and a guard class that permits the transfer of network traffic (communication transaction)(col. 17, lines 32-40). Sheldon discloses of a firewall that enforces security policies by monitoring traffic from outside the network such as the Internet (untrustworthy network) addressed to the internal network (trustworthy network) and selectively preventing the transfer of traffic (communication transactions) by applying security policies (protection rules)(pg 3 & 7). Please refer to motivation as recited above for reasons to combine the teachings of Sheldon as applied to Nessett et al.

As per claims 4 and 13, Nessett et al discloses that updates to the security policy statements (protection rules) are selectively transferred from the network management station's (server) database to the firewalls (portals) across the Internet (untrustworthy network)(col. 9, lines 17-32 & col. 10, lines 28-31). An administrator (human expert) manages the security policy management system (server)(col. 6, lines 17-22).

As per claims 9 and 18, the combined teachings of Nessett et al and Sheldon are relied upon for disclosing of controlling network traffic (col. 3, lines 53-54) and that a security policy dictates the way the network devices should accept or deny traffic (communication transaction) according to the firewall (portal)(col. 17, lines 32-40). It is interpreted by the examiner that the teachings of Nessett et al select between two

classes for security policies (protection rules) when applied to monitoring traffic, namely an exclusion class that denies network traffic (communication transaction) and a guard class that permits the transfer of network traffic (communication transaction)(col. 17, lines 32-40). An administrator (human expert) manages the security policy management system (server)(col. 6, lines 17-22) as is disclosed by Nessett et al.

Sheldon discloses of a firewall that enforces security policies by monitoring traffic from outside the network such as the Internet (untrustworthy network) addressed to the internal network (trustworthy network) and selectively preventing the transfer of traffic (communication transactions) by applying security policies (protection rules)(pg 3 & 7).

4. Claims 5-8 and 14-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al, U.S. Patent 5,968,176 in view of Sheldon in further view of Joyce, U.S. Patent 6,519,703.

As per claims 5-7 and 14-16, the combined teachings of Nessett et al and Sheldon are relied upon for disclosing of controlling network traffic (col. 3, lines 53-54) and that a security policy dictates the way the network devices should accept or deny traffic (communication transaction) according to the firewall (portal)(col. 17, lines 32-40). It is interpreted by the examiner that the teachings of Nessett et al select between two classes for security policies (protection rules) when applied to monitoring traffic, namely an exclusion class that denies network traffic (communication transaction) and a guard class that permits the transfer of network traffic (communication transaction)(col. 17, lines 32-40) as is disclosed by Nessett et al. Sheldon discloses of a firewall that enforces security policies by monitoring traffic from outside the network such as the

Art Unit: 2131

Internet (untrustworthy network) addressed to the internal network (trustworthy network) and selectively preventing the transfer of traffic (communication transactions) by applying security policies (protection rules)(pg 3 & 7). The combined teachings of Nessett et al and Sheldon are silent in disclosing of the use and expert system to analyze and construct a new protection rule when detecting a new security threat. It is disclosed by Joyce of a heuristic firewall that uses an expert system to detect attacks (security threats) and to detect new attacks (security threats) by adaptability to the firewall rule base (protection rules)(col. 2, lines 20-29). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply expert systems as a means of detecting new forms of attacks and to further report them so that they can be detected in further attempts. Joyce recites problems in the prior art with firewalls in that they are static in nature and are limited to how a firewall administrator has programmed the firewall and cannot learn and adapt to data that flows (col. 1, lines 21-34). It is obvious that the combined teachings of Nessett et al and Sheldon would have benefited from the teachings of Joyce by overcoming problems in the prior art whereby firewalls are limited in nature since the prior art firewall is static and by implementing a firewall with the use of a expert system allows for the ability to detect new forms of attacks.

As per claims 8 and 17, Joyce et al discloses of an expert system being guided by an administrator (human expert)(col. 2, lines 24-26, col. 2, line 66 through col. 3, line 3, & col. 4, lines 61-66). Please refer to motivation as recited above for reasons to

Art Unit: 2131

combine the teachings of Joyce as applied to the combination of Nessett et al and Sheldon.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Beebe et al, U.S. Patent 6,226,372; Centralized security manager that collects updates from remotely located firewalls and distributes policy updates to remotely located firewalls.

Shwed, U.S. Patent 5,606,668; Demonstrates a general teaching of a firewall and its capabilities.

Watchguard, "Protecting the Internet Distributed Enterprise"; Centralized management of remote devices.

Bellovin et al, "Network Firewalls"; General firewall teaching.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 703-305-1843. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

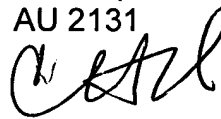
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak

AU 2131



2/8/04

CR



February 8, 2004